Цель работы

Освоить на практике разложение чисел на множители.

Выполнение лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий p-метод Полларда

p-метод Полларда

Метод Полларда применяется при факторизации натуральных чисел.

Основные шаги:

Вход: число N, начальное значение c, функция f, обладающая сжимающими свойствами Выход: нетривиальный делительно числа n

1. положить a <- c, b <- c
2. Вычислить a Б- f(a)(mod n), b <- f(b) (mod n)
3. Найти d <- НОД(a-b, n)
4. Если 1< d< n, То положить p <- di результат: p. При d=n результат: "Делитель не найден"; при d=1 вернуться на шаг 2

Чтобы реализовать программу, был написан след. код на python:

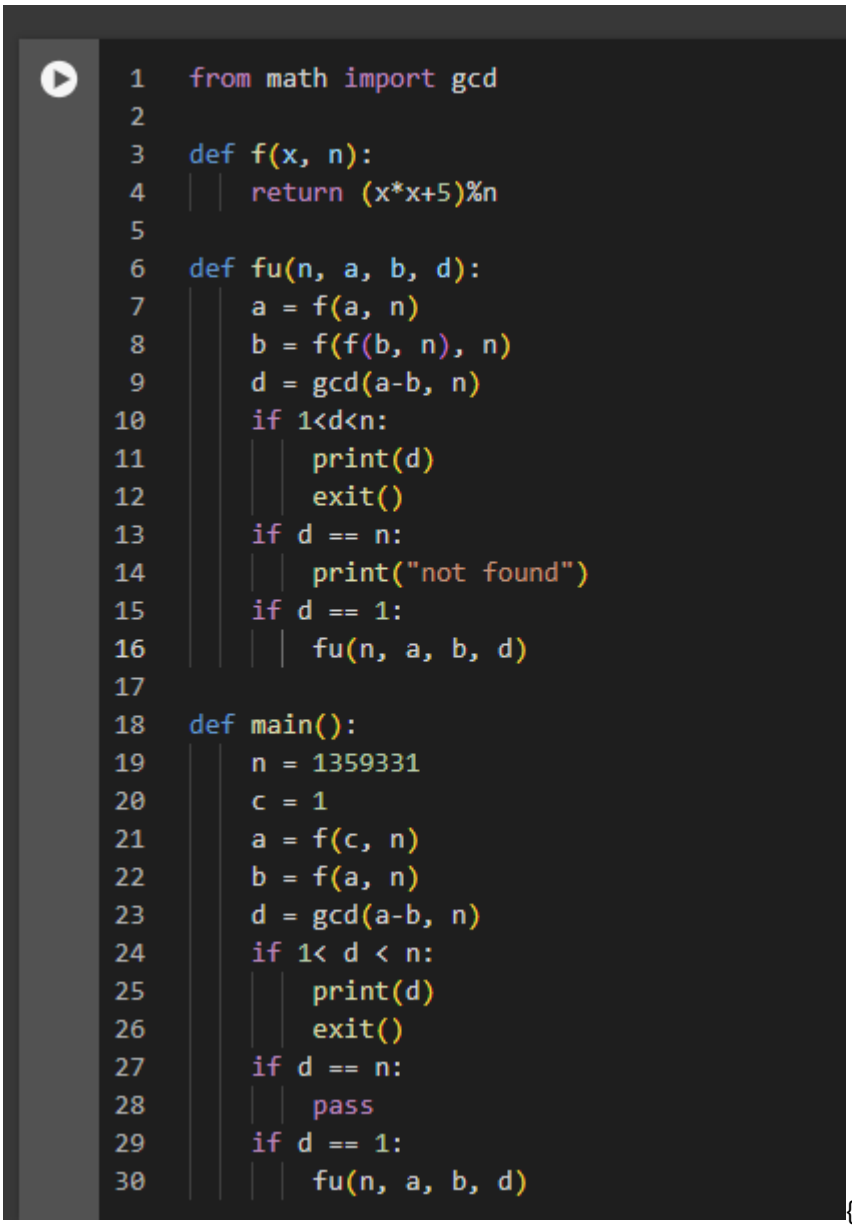
1. Функция, реализующая p-метод Полларда
2. Функция нахождения НОД [@fig:1].

```python
from math import gcd

def f(x, n):
    return (x*x+5)%n

def fu(n, a, b, d):
    a = f(a, n)
    b = f(f(b, n), n)
    d = gcd(a-b, n)
    if 1<d<n:
        print(d)
        exit()
    if d == n:
        print("not found")
    if d == 1:
        fu(n, a, b, d)

def main():
    n = 1359331
    c = 1
    a = f(c, n)
    b = f(a, n)
    d = gcd(a-b, n)
    if 1< d < n:
        print(d)
        exit()
    if d == n:
        pass
    if d == 1:
        fu(n, a, b, d)
```

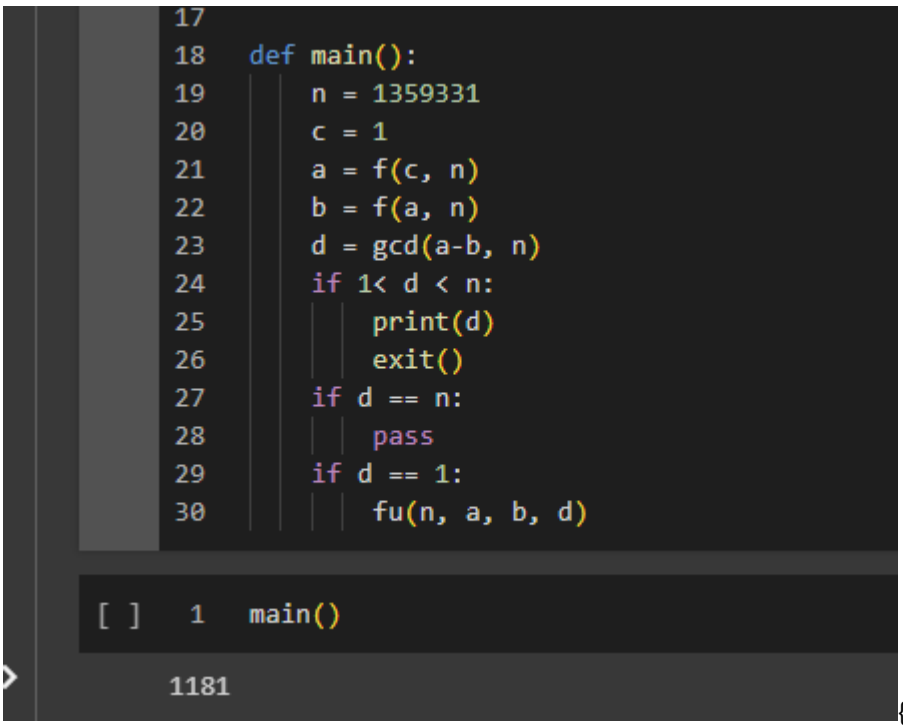
 {#fig:1 width=100%}

Выходные значения программы (пример из методички) [@fig:2].

```python
def main():
    n = 1359331
    c = 1
    a = f(c, n)
    b = f(a, n)
    d = gcd(a-b, n)
    if 1< d < n:
        print(d)
        exit()
    if d == n:
        pass
    if d == 1:
        fu(n, a, b, d)
```

```
[ ]  main()

1181
```

 {#fig:2 width=100%}

Выводы

В результате выполнения работы освоили на практике алгоритм разложения чисел на множители.

Список литературы

1. Методические материалы курса